Technisch & organisatorische Maßnahmen

gemäß Art. 32 DSGVO

Zusätzlich zu den im Datenschutzkonzept beschriebenen Maßnahmen wird eine Vielzahl von konkreten Schutzmaßnahmen getroffen. Somit werden die Forderungen der DSGVO nach geeigneten technische und organisatorische Maßnahmen und die Gewährleistung eines dem Risiko angemessenes Schutzniveau erfüllt werden.

Diese TOM wurde zuletzt geändert am 01.04.2022 um 13:30:00.

litfax® GmbH - Verlag für Banken
Sitz der Gesellschaft: Berlin
Darßer Bogen 3 - 13088 Berlin

Telefon: +49 (0) 30 / 688 1919-70
Telefax: +49 (0) 30 / 688 1919-99
E-Mail: info@my-litfax.de

Vertreten durch:
Peter Junge

Registereintrag:
Eingetragen im Handelsregister.
Registergericht: Berlin
Registernummer: HRB 96160B

Umsatzsteuer-ID:
Umsatzsteuer-Identifikationsnummer nach §27a Umsatzsteuergesetz: DE241211663

Die vorliegenden technischen und organisatorischen Maßnahmen wurden durch die Geschäftsführung (Peter Junge) genehmigt.

Datenschutzbeauftragter: DataCo GmbH

Inhalt

Technisch-Organisatorische Maßnahmen

Vorwort

Das Dokument beschreibt die als verbindlich festgelegten technischen und organisatorischen Maßnahmen im Zusammenhang mit durchgeführten Auftragsverarbeitungsvorgängen zwischen Auftraggeber und Auftragnehmer. Die dargestellten Maßnahmen stellen somit ein Abbild des gelebten Datenschutz- und Datensicherheitskonzept des Standortes dar.

Datenschutz- und Datensicherheitskonzept

Der folgende Maßnahmenkatalog beschreibt die im Rahmen der Auftragsverarbeitung zu treffenden technischen und organisatorischen Einzelmaßnahmen nach Art. 24 Abs. 1 EU-DS-GVO. Die EU-DS-GVO verpflichtet Unternehmen die Datenverarbeitung personenbezogener Daten durch angemessene, technische und organisatorische Maßnahmen abzusichern und personenbezogene Daten nach Möglichkeit zu pseudonymisieren. Die getroffenen Maßnahmen müssen dabei dem Risiko des jeweiligen Datenverarbeitungsvorgangs Rechnung tragen und dem derzeitigen Stand der Technik entsprechen. Diese Anforderungen erfüllt der Auftragnehmer durch ein wirksames Zusammenspiel aus Datenschutzmanagement und Informationssicherheitsmanagement und hat angemessene Maßnahmen zur Absicherung der Datenverarbeitungsvorgänge getroffen. Insbesondere die Schutzwerte: Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit. Den Schutzwerten werden dabei folgende informationssicherheitsrelevanten Definitionen zugrunde gelegt:

- Vertraulichkeit: Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen.
- Integrität: Der Begriff Integrität bezieht sich auf die Korrektheit der verarbeiteten Informationen und Daten.
- Verfügbarkeit: Der Begriff der Verfügbarkeit bezieht sich auf Informationen, Daten, Applikationen sowie Systeme und betrifft deren Funktionsfähigkeit bzw. Abrufbarkeit.
- Belastbarkeit: Die Belastbarkeit stellt als besonderen Aspekt der Verfügbarkeit die Anforderung, dass Systeme auch im Störfall, Fehlerfall oder bei hoher Belastung möglichst widerstandsfähig ausgestaltet sein müssen.

I. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Server:
In den Unternehmensräumlichkeiten werden ein oder mehrere Server eingesetzt.

Server - Externer Einsatz:
Im Unternehmen werden externe Server (z.B. in einem Rechenzentrum) angemietet.

Server - Räumlichkeiten:
Die im Unternehmen eingesetzten Server werden in einem speziell dafür vorgesehenem Raum betrieben.

Server - Zutrittsberechtigung:
Im Unternehmen ist der Zutritt zu den Serverräumen auf den minimal benötigten Personenkreis beschränkt.

Server - Zutrittskontrolle:
Im Unternehmen wird ein Zutrittskontrollsystem zum Serverraum eingesetzt.

Sicherung des Unternehmensgeländes - Abgrenzung:
Das Unternehmensgelände / die Unternehmensräumlichkeiten werden vom öffentlichen Bereich abgegrenzt durch:
- Zaun, Tor und abschließbare Türen

Sicherung des Unternehmensgeländes - Alarmanlage:
Das Unternehmensgelände und ggfs. Teile davon werden durch eine Alarmanlage gesichert.

Zutrittskontrollsystem:
Im Unternehmen wird ein zentral verwaltetes Zutrittskontrollsystem eingesetzt.

Zutrittskontrollsystem - Abschließbare Räume:
Im Unternehmen sind sämtliche Räume, in denen ein Zugriff auf personenbezogene Daten möglich ist, abschließbar.

Zutrittskontrollsystem - Besucheranmeldung:
Im Unternehmen wird die Anwesenheit von Besuchern angemeldet über:
- Besucherbuch

Zutrittskontrollsystem - Technisches Mittel:
Das Zutrittskontrollsystem basiert auf folgenden technischen Mitteln: - Schlüssel

Zutrittskontrollsystem - Verwaltung:
Das Zutrittskontrollsystem wird folgendermaßen verwaltet:
- Schlüsselbuch

II. Zugangskontrolle
Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Fernwartung - Tools:
Im Unternehmen werden folgende Tools zur Fernwartung eingesetzt:
- TeamViewer

Fernwartung - VPN:
Im Unternehmen wird zur Fernwartung ein VPN-Tunnel eingesetzt.

Mitarbeiter - Aufbewahrung sensibler Informationen:
Im Unternehmen sind die Beschäftigten verpflichtet worden, personenbezogene Daten bei Verlassen des Arbeitsplatzes verschlossen zu lagern (sog. Clean-Desk-Policy).

Tragbare Endgeräte - Passwortkomplexität:
Im Unternehmen werden ausreichend komplexe Passwörter und PINs, für die Nutzung von tragbaren Endgeräten gefordert.

Tragbare Endgeräte - Zugangssperren:
Im Unternehmen verfügen tragbare Endgeräte über Zugangssperren (Passwort, PIN, Muster o. A.).

Zugang zu personenbezogenen Daten in Bereichen mit Publikumsverkehr:
Im Unternehmen wird dafür gesorgt, dass personenbezogene Daten in Bereichen mit Publikumsverkehr nicht frei zugänglich sind.

III. Zugriffskontrolle
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können.

Administratoren - Vergabe von Zugangs- und Zugriffsberechtigungen:
Im Unternehmen erfolgt die Vergabe von Zugangs- und Zugriffsberechtigungen anhand der Funktion der Zugangs- bzw. Zugriffsberechtigten.

Administratoren - Vorübergehende Sperrung von Zugangs- und Zugriffsberechtigungen:
Im Unternehmen erfolgt eine vorübergehende Sperrung von Zugangs- bzw. Zugriffsberechtigungen bei längeren Abwesenheiten.

Ausgeschiedene Personen - Entzug von Berechtigungen:
Im Unternehmen wird sichergestellt, dass sämtliche Zugangsberechtigungen und Zugriffsberechtigungen einer ausscheidenden Person zeitnah gesperrt und ggf. gelöscht werden.

IT-Sicherheit - Firewall:
Im Unternehmen wird eine bzw. mehrere Firewalls gegen unerwünschte Netzwerkzugriffe eingesetzt.
Im Unternehmen werden folgende Firewalls eingesetzt:
- Sophos

IV. Datenträgerkontrolle

Es ist zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Datenträgermanagement - Bestandsverzeichnis:
Im Unternehmen wird für folgende elektronischen Datenträger ein Bestandsverzeichnis geführt:
- Laptops
- - Mobiltelefone
- - Tabletcomputer

Tragbare Datenträger - Verschließbare Behältnisse:
Im Unternehmen stehen an allen Arbeitsplätzen verschließbare Behältnisse zur Verfügung, um Unterlagen und Datenträger sicher aufbewahren zu können.

V. Übertragungskontrolle

Es ist zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können.

Telekommunikation - Verbindung zum Telekommunikationsprovider:
Zur Verbindung mit dem Telekommunikationsprovider wird folgende Methode verwendet:
- Reguläre DSL/Glasfaserverbindung

VI. Transportkontrolle

Es ist zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Datenübertragung - Berechtigter Zugriff:
Im Unternehmen werden beschriebene Datenträger vor und nach dem Versand so aufbewahrt, dass ein Zugriff nur für berechtigte Personen möglich ist.

Datenübertragung - Unkenntlicher Transport:
Im Unternehmen werden Behältnisse, die dem Transport von Datenträgern mit personenbezogenen Daten dienen, nicht als solche beschriftet.

VII. Benutzerkontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können.

Ausgeschiedene Personen - Rückforderung unternehmenseigener Gegenstände:
Im Unternehmen wird sichergestellt, dass sämtliche unternehmenseigene Gegenstände mit Bezug zu personenbezogenen Daten von einer ausscheidenden Person zurückgefordert werden.

Mitarbeiter - Maßnahmen:
Um im Unternehmen die Beschäftigten auf die Wichtigkeit des Datenschutzes hinzuweisen und diese gemäß den Erfordernissen zu verpflichten, werden folgende Maßnahmen getroffen:
- Verpflichtung der Beschäftigten zu Verhaltensregeln
- Verpflichtung der Beschäftigten auf das Datengeheimnis

Mitarbeiter - Schulungen:
Um die Mitarbeiter auf die Wichtigkeit des Datenschutzes hinzuweisen und diese gemäß den Erfordernissen zu verpflichten, werden folgende Maßnahmen getroffen:
- Schulung aller zugriffsberechtigten Beschäftigten

Schulungen für Beschäftigte - Regelmäßigkeit:
Im Unternehmen finden regelmäßig Schulungen zum Thema Datenschutz statt.

VIII. Auftragskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Dienstleister Datenträgerentsorgung:
Es wird ein externer Dienstleister zur Entsorgung von Datenträgern genutzt.

Dienstleister Datenträgerentsorgung - Zertifizierung:
Der externe Dienstleister besitzt folgende Zertifizierung:
- DIN 66399

Externe Dienstleister:
Das Unternehmen arbeitet mit externen Dienstleistern zusammen.

Externe Dienstleister - Kontakt zu personenbezogenen Daten:
Im Unternehmen werden externe Dienstleister, welche in Kontakt mit personenbezogenen Daten gelangen könnten, stets bei der Tätigkeit überwacht.

Externe Dienstleister - Weisungen zur Verarbeitung:
Im Unternehmen werden Weisungen zur Verarbeitung personenbezogener Daten ausschließlich schriftlich an Auftragsverarbeiter erteilt.

IX. Speicherkontrolle

Die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter, personenbezogener Daten ist zu verhindern.

Authentifizierung - Datensperrung und -löschung:
Im Unternehmen besteht die Möglichkeit auf Antrag personenbezogene Daten zu sperren und zu löschen.

Automatische Bildschirmsperre:
Im Unternehmen wird eine automatische Bildschirmsperre eingesetzt.

Automatische Bildschirmsperre - Zeitraum:
Im Unternehmen wird die automatische Bildschirmsperre nach maximal 10 Minuten aktiviert.

Kamerabilder/Videoüberwachung - Zugriff:
Folgende Positionen haben Zugriff auf die Bilder:
- Geschäftsführung

Mitarbeiter - Fachgerechte Entsorgung personenbezogener Daten:
Im Unternehmen sind die Beschäftigten angehalten personenbezogene Daten fachgerecht zu entsorgen.

Verschlüsselung der Übertragung:
Daten werden bei der Übertragung verschlüsselt.

X. Verfügbarkeitskontrolle

Es ist zu gewährleisten, dass personenbezogene Daten jederzeit verfügbar sind und besonders gegen zufällige Zerstörung oder Verlust geschützt sind.

Archivierungskonzept - Gesetzliche Aufbewahrungspflicht:
Es liegt keine gesetzliche Aufbewahrungspflicht für die archivierten Dokumente vor.

Server - Gefahrenabsicherung:
Die Serverräume wurden gegen folgende Gefahren abgesichert:
- Wasser
- Sabotage
- Feuer

Unterbrechungsfreie Stromversorgung:
Im Unternehmen wird eine unterbrechungsfreie Stromversorgung eingesetzt.

Unterbrechungsfreie Stromversorgung - Überbrückungsdauer:
Die unterbrechungsfreie Stromversorgung kann folgenden Zeitraum überbrücken:
- ca. 30min

Unterbrechungsfreie Stromversorgung - Überprüfung nach Änderungen:
Im Unternehmen wird die Leistung der unterbrechungsfreien Stromversorgung erneut geprüft, wenn Änderungen an der Hardware vorgenommen wurden.

XI. Zuverlässigkeit

Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust abgesichert sind.

IT-Sicherheit - Software Aktualisierungen:
Aktualisierungen werden zeitnah wie folgt umgesetzt:
- Automatisiert

IT-Sicherheit - Trennung der Netzwerke:
Das Netzwerk zur Videoüberwachung ist wie folgt in verschiedene Segmente aufgeteilt:
- Physisch getrennt

Kamerasoftware - Updates:
Es werden regelmäßig Updates der Kamerasoftware durchgeführt.

XII. Wiederherstellbarkeit

Es ist zu gewährleisten, dass personenbezogene Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Sicherungen:
Im Unternehmen werden die Sicherungen durchgeführt von: - Eigenständige Backups (z. B. durch NAS-System)

XIII. Trennbarkeit

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Trennung von Arbeitsplätzen:
Im Unternehmen werden Arbeitsplätze zur Verarbeitung besonderer Kategorien personenbezogener Daten räumlich von anderen Arbeitsplätzen getrennt.

XIV. Betriebssystem

Es ist zu verhindern, dass Unbefugte Zugriff auf Betriebssysteme erhalten können.

Passwortschutz - Benutzerkonten:
Auf Betriebssystemebene wird jedes Benutzerkonto des Betriebssystems durch ein Passwort geschützt.

Passwortschutz - Passwortkomplexität:
Auf Betriebssystemebene gibt es eine Vorgabe für die Passwortkomplexität.